SPECIFICATION AMENDMENTS

Please replace the title at the top of page 1 with the following amended title:

ESTABLISHING A NEW SHARED SECRET KEY OVER A BROADCAST CHANNEL FOR A MULTICAST GROUP BASED ON AN OLD SHARED SECRET KEY

Please add the following section heading and new paragraph on page 1 immediately after the amended title and before the section titled "FIELD OF THE INVENTION":

RELATED APPLICATIONS

A1

This application is related to: (1) co-pending non-provisional application Ser. No. 10/715,932 (Attorney Docket No 50325-0854), filed November 17, 2003, entitled "Operational Optimization of a Shared Secret Diffie-Hellman Key Exchange Among Broadcast or Multicast Groups," naming Sunil K. Srivastava as inventor, and (2) co-pending non-provisional application Ser. No. 10/715,721 (Attorney Docket No. 50325-0855n), filed November 18, 2003, entitled "Processing Method for Key Exchange Among Broadcast or Multicast Groups that Provides a More Efficient Substitute for Diffie-Hellman Key Exchange," naming Sunil K. Srivastava as inventor.

Please replace the paragraph on page 14, lines 1-5 with the following amended paragraph:

A2

As depicted in FIG. 3B, after the initial multicast group 304 is established, a second user (Bob 306) requests to join the multicast group 304. In one embodiment, to request access, Bob 306 chooses a random integer y and computes an exchange key Y', where $Y' = g^y \bmod n$. For purposes of illustrating an example, assume that the value chosen by Bob 306 for random number y is "13". Thus, the value of exchange key Y' is calculated by ~~Alice 302~~ Bob 306 as:

Please replace the paragraph on page 14, lines 15-21 with the following amended paragraph:

If the multicast group 304 determines that Bob 306 is to be admitted, one of the multicast group members (in this example, Alice 302) responds to a request for admission by Bob 306 ~~request~~ by transmitting a response 310 that includes the exchange key K' of the multicast group. In addition, each member of the multicast group 304 uses the exchange key Y' to generate a new shared secret key k1, where $k1 = (Y'^{k} \bmod (n))$, for communicating with other members of the group. Thus, the value of the new shared secret key k1 is calculated by multicast group 304 as follows:

Please replace the paragraph on page 16, lines 3-7 with the following amended paragraph:

If the multicast group 312 determines that Carol 314 is to be admitted, one of the multicast group members (in this example, either Alice 302 or Bob 306) responds to the request of Carol 314 ~~request~~ by transmitting a response 318 that includes the multicast group's 312 exchange key K1', where $K1' = (g^{k1} \bmod (n))$. For example, K1' equals $(5^{408} \bmod (563) = 541)$.